tenable.ot™

SOLUTION OVERVIEW

FORTINET JOINT SOLUTION BRIEF

BUSINESS CHALLENGE

Industrial Control Systems (ICS) quite literally control our lives. While it was once isolated from any other part of the organization or network and considered static systems, this is no longer the case. ICS devices which are on the OT network are connected to IT systems. This means that the malware, cyber-attacks, insider threats, misconfigurations and even failed maintenance which impact one area of the organization can easily propagate to the other.

Today's attacks are significantly more sophisticated and include zero-day and targeted attacks, social engineering, and spear phishing—all designed to establish a beachhead and modify or destroy critical industrial operations. The key to a successful breach is to keep the nefarious activity undetected for as long as possible.

Unlike IT networks, Industrial Control Systems lack a proper foundation for securing the infrastructure. Most devices don't require authentication, making it difficult to prevent unauthorized access or changes to critical devices. In addition, there are no event logs or historical data to help with event detection and response. Without this proper foundation of visibility and control, added challenges emerge in managing assets, detecting threats, and managing systems configurations in OT environments.

SOLUTION

Some of the most effective tools for fighting attacks involve maintaining strict security policies while still allowing critical operational activities to execute unimpeded. Security administrators face the challenge of managing appropriate access, rulesets, and device states across the IT and OT environments.

Tenable.ot and Fortinet's FortiGate provide a joint solution designed to eliminate the traditional IT-OT security silos by integrating with the security, work flow, incident response and recovery procedures that can span across both environments. The partnership between Tenable and Fortinet's Fabric Ready Partner Ecosystem provides customers with a seamless solution to collect, analyze and report on all devices and activity. This helps reduce the time it takes to identify security related issues within the converged IT/OT infrastructure. This includes Industrial Controller and device activity, who is accessing files, what privileged user activity is taking place, and what potential threats exist on devices and in the network.

FORTINET®

TECHNOLOGY COMPONENTS

- Tenable.ot
- Fortinet FortiGate

KEY BENEFITS

The joint partnership between Tenable and Fortinet's Fabric Ready Partner Ecosystem offers visibility, security and control for industrial networks, enabling security professionals to effectively detect and mitigate threats to the safety, reliability and continuity of industrial processes. As part of the joint solution, monitoring occurs across the IT and OT environments to ensure early and comprehensive threat detection and mitigation that other point products can easily miss. Specifically,

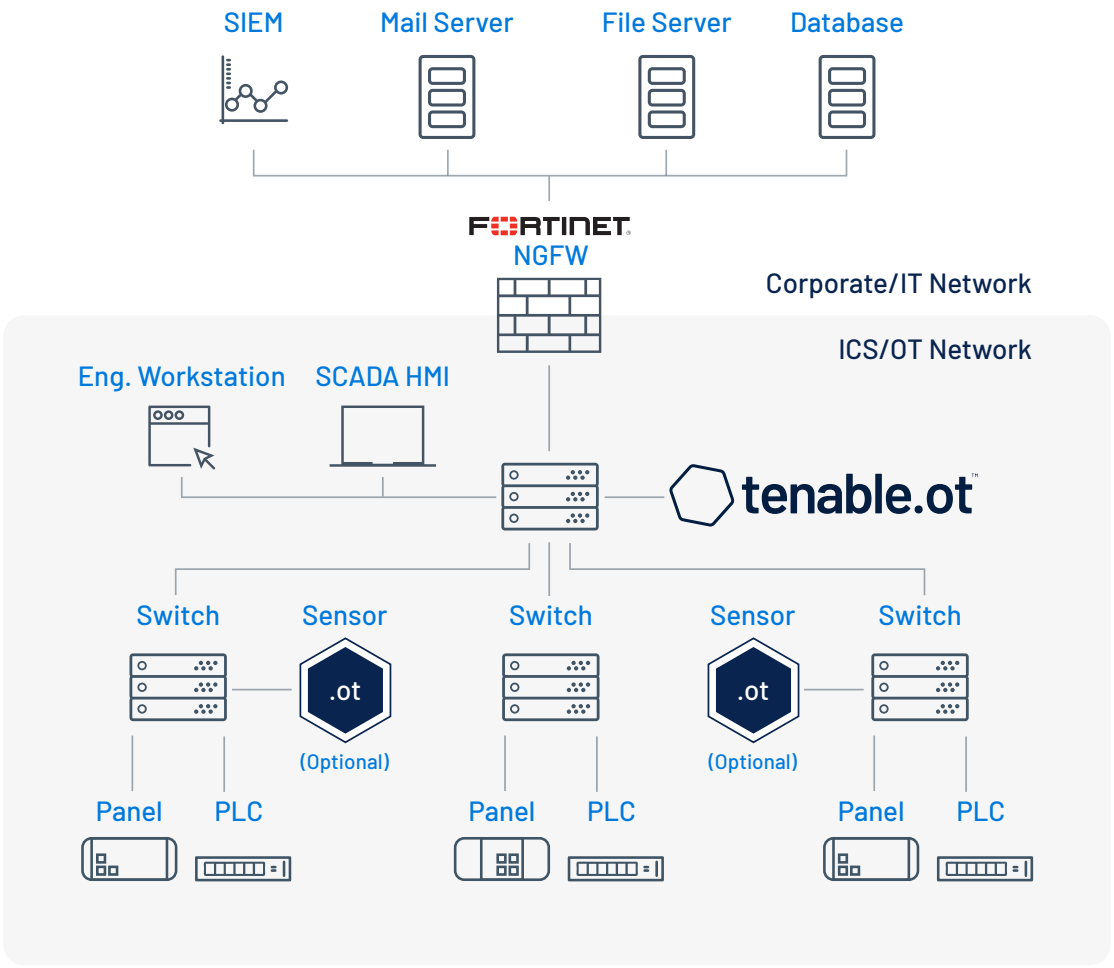
- Improved security automation, sensing and visibility
- Increased control over distributed operations
- Better compliance with regulatory requirements and tracking
- Higher responsiveness when incidents occur and improved organizational performance
- Better decision making based on more detailed information
- Proactive maintenance and reduced response times to unforeseen disruptions
- Improved flow of information to stakeholders

KEY COMPONENTS

How It Works

FortiGate enterprise firewalls offer flexible deployments from the network edge to the core, data center, internal segment, and the Cloud. FortiGate enterprise firewalls leverages purpose-built security processors (SPUs) that delivers scalable performance of advanced security services like Threat Protection, SSL inspection, and ultra-low latency for protecting internal segments and mission critical environments. FortiGate NGFW provides automated visibility into cloud applications, IoT devices and automatically discovers end to end topology view of the enterprise network. FortiGate is a core part of security fabric and validated security protect the enterprise network from known and unknown attacks.

Tenable.ot provides situational awareness and real-time security for industrial control networks to ensure operational continuity and reliability. It delivers comprehensive visibility and oversight into all OT activities, whether they are network or device based. These include changes to controller logic, configuration and state across all vendor devices, network communication patterns, rouge devices, malware propagation, and more. This is done via both the Deep Packet Inspection engine of proprietary control communications, and patented active querying technology by utilizing native communication protocols without ever affecting them. The result is validation of PLC and PCs firmware/OS, code/software and configuration. The joint integration allows users to leverage Tenable.ot generated events and automatically create firewall rules (enforcement policies) on the FortiGate NGFW in order to block unwanted or malicious activity.



ABOUT TENABLE

Tenable®, Inc. is the Cyber Exposure company. More than 30,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 30 percent of the Global 2000 and large government agencies. Learn more at www.tenable.com.

ABOUT FORTINET

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers our customers with complete visibility and control across the expanding attack surface and the power to take on ever-increasing performance requirements today and into the future. Only the Fortinet Security Fabric platform can address the most critical security challenges and protect data across the entire digital infrastructure, whether in networked, application, multi-cloud or edge environments. Learn more at www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

AVAILABLE POLICIES WITH THE INTEROPERABILITY

Tenable.ot enables OT engineering and security professionals to configure their own

policies or fine tune existing policies from the vast library to alert for specific activities as well as for various anomalies in the ICS network. Each policy includes the conditions by which an alert will be triggered as well as the actions taken following an alert.

The type of policies that can be used to generate policies on the FortiGate NGFW are:

- Baseline Deviation
- Unauthorized Conversation
- Intrusion Detection

Controller Activities relate to the activities in the network (i.e. the engineering commands that impact controllers' state and configuration). It is possible to define specific activities that always generate alerts or to designate a set of criteria for generating alerts. For example, if certain activities are performed at certain times and/or on certain controllers. Both black listing and white listing of assets, activities and schedules are supported.

Controller Validation relate to changes that take place to the controllers in the network. This can involve changes in the state of a controller as well as changes to the firmware, asset properties, hardware/module change or code blocks (done over the network or locally on the device). The policies can be limited to specific schedules (i.e. firmware upgrade during a work day), and/or specific controller/s.

Network Events & Threats relate to the network assets and the communication streams between assets. This includes assets that were added to or removed from the network and includes traffic patterns that are anomalous for the network or that have been flagged as a cause for concern. For example, if an engineering station communicates with a controller using a protocol that is not part of a pre-configured set of protocols. These policies can be limited to specific schedules and/or specific assets.

SCADA Events detect changes in set-point values which can harm the industrial process. These changes may result from a cyber-attack or human error.

For support please contact: support@tenable.com

tenable®

COPYRIGHT 2021 TENABLE, INC. ALL RIGHTS RESERVED. TENABLE, TENABLE.IO, TENABLE NETWORK SECURITY, NESSUS, SECURITYCENTER, SECURITYCENTER CONTINUOUS VIEW AND LOG CORRELATION ENGINE ARE REGISTERED TRADEMARKS OF TENABLE, INC. TENABLE.SC, TENABLE.OT, LUMIN, INDEGY, ASSURE, AND THE CYBER EXPOSURE COMPANY ARE TRADEMARKS OF TENABLE, INC. ALL OTHER PRODUCTS OR SERVICES ARE TRADEMARKS OF THEIR RESPECTIVE OWNERS.